IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IRENE SIMMONS AND RODELL SANDERS, for themselves and others similarly situated,	)	Case No. 1:20-cv-1128
Plaintiffs,	)	Judge John J. Tharp Jr.
v.	)	Magistrate Judge Jeffrey I. Cummings
MOTOROLA SOLUTIONS, INC., and VIGILANT SOLUTIONS, LLC,	)	
Defendants.	)	

DEFENDANTS' REPLY IN SUPPORT OF
AMENDED MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Introduction

Plaintiffs' opposition brief confirms that this is an ill-considered BIPA case, and one that does not withstand summary judgment. BIPA does not apply to government contractors when they are working for government entities. 740 ILCS 14/25(e). Plaintiffs avoided dismissal at the pleading stage only by alleging falsely that Defendants sold access to biometric data about Plaintiffs to "private companies" in addition to Defendants' government customers. (Dkt. 6, Amend. Compl. ¶ 36; Dkt. 33, Order on Mot. to Dismiss at 3.) But now, on summary judgment, Plaintiffs are unable to support that allegation with any genuine evidence. In contrast, Defendants' witnesses, corroborated by documents, have testified unrebutted that Defendants contracted only with law enforcement agencies and other government customers—not private companies—to provide access to the electronic booking photo gallery that contained alleged biometric information about Plaintiffs. As Defendants' corporate representative testified: "I'm saying to a certainty that we never provided access to jail booking photos, sexual predator photos, or Crime Stopper data to anybody other than law enforcement and government agencies." (Dkt. 129-18, Pls. RSOF Ex. 18, 30(b)(6) Tr. at 98:9–13.) There is no contrary evidence and thus no triable issue.

In their opposition, Plaintiffs largely ignore the undisputed fact that Defendants have served hundreds of law enforcement agencies and other public authorities by providing access to facial recognition tools and the booking photo gallery, just as BIPA's Section 25(e) contemplates. But three points are dispositive: (a) Defendants were contractors working for government authorities to provide facial recognition technologies before September 30, 2014; (b) Defendants did not collect or come to possess alleged biometric information pertaining to either Plaintiff until September 30, 2014, after they were working pursuant to those contracts; and (c) since that time, Defendants have contracted only with government authorities—not private parties—to provide

access to the booking photo gallery that contains information about the Plaintiffs. (Dkt. 112, Mot. at 10–11.)

Plaintiffs attempt to cast doubt on each of those points, but they can muster only out-of-context snippets of documents and speculation, not any genuine factual dispute. In particular:

Timing of contracts. Plaintiffs do not dispute that the Wilmette Police Department signed and accepted a quotation from Vigilant for facial recognition technology including a "[f]acial [r]ecognition gallery" on September 25, 2014, but they quibble that Vigilant apparently neglected to sign the accompanying contract after the Wilmette PD signed it. (Dkt. 136, Opp. at 1, 16.) There is no genuine question, however, that Vigilant and the Wilmette PD were contractually bound. Plaintiffs themselves even adduce evidence that the Wilmette PD *paid* Vigilant about two months after signing. (*Id.* at 16.) Vigilant similarly contracted with the Beaumont, California Police Department. (*See* Mot. at 5; Dkt. 140, Colón Decl. ¶ 4.) Plaintiffs argue that Defendants did not attach the Beaumont PD contract to their moving papers (Opp. at 17), but Defendants produced the executed June 24, 2014 Project Quotation and the executed September 23, 2014 Enterprise Services Agreement. (Dkt. 114-2; Dkt. 140-2 at Motorola 50106.) There is thus no genuine dispute that Vigilant was a contractor working for government authorities to provide facial recognition technology, including access to the booking photo gallery, by September 2014.

Timing of photos. Defendants' records show that they did not gather any information from a booking photo of Plaintiff Sanders before September 30, 2014, *i.e.*, after Vigilant was working pursuant to the above contracts. (Dkt. 114, Olive Decl. ¶ 12.) Plaintiffs nonetheless argue that Vigilant *might* have obtained a photo of Plaintiff Sanders and gathered information from it earlier, but they admit that there is "no direct evidence" for that conjecture. (Opp. at 14.) Plaintiffs instead attempt to string together speculative "inferences" that a photo of Plaintiff Sanders was included in an earlier photo set supplied by a different vendor, but this boils down to an unsupported guess

that because his photo was in a later set of photos, it must have been in an earlier set of photos from a different source. Plaintiffs also ignore undisputed proof that the earlier set of booking photos was from only Texas and Florida, while any photo of Plaintiff Sanders was from Illinois. (*See* Pls. RSOF Ex. 18, 30(b)(6) Tr. 77:2–13, 78:20–23; 79:12–80:11, 100:14–21.) Plaintiffs do not even mention Plaintiff Simmons in their brief (thus waiving her claims), and do not contend that Defendants possessed her booking photo before September 2014. (*See* Opp. at 13–15.)

No private customers for booking photo gallery. Defendants provided Plaintiffs with sworn testimony, sales spreadsheets, and copies of agreements establishing that they have contracted with more than one thousand government agencies—not private entities—to provide access to facial recognition tools and the booking photo gallery. Ignoring that, Plaintiffs attempt to seize upon generalized language in some of Defendants' marketing materials about private customers like banks. But, on their face, those documents refer to *products that did not include access to the booking photo gallery*, which is the database that contained the information about Plaintiffs that is the basis of this lawsuit. Vigilant sells search tools that private companies may use to search their own "watchlists" of photos, but it contracts only with government customers to provide access to the booking photo gallery. (Pls. RSOF Ex. 18 30(b)(6) Tr. at 98:9–13.)

Indeed, when it comes to actually identifying any alleged private customer for the booking photo gallery, Plaintiffs point to only two—a bank in Ukraine called Prominvestbank and the owner of the Indianapolis Motor Speedway—but those entities did not purchase such access, and there is no genuine evidence they did. Prominvestbank, a bank located in Europe, did not purchase access to a gallery of booking photos from the United States; Plaintiffs have simply misread a line on a spreadsheet. (*See* Dkt. 141, Garoutte Decl. ¶ 7). And the contract concerning the Indianapolis

Motor Speedway was with the *police department* in Speedway, Indiana, where the racetrack is located.[1] (Dkt. 140-1, Motorola 8401 at 8419; Dkt. 142, Workman Decl. ¶¶ 3–4.)

In short, Plaintiffs cannot identify evidence that Defendants collected, captured, purchased, received through trade, otherwise obtained, or possessed any alleged biometric information of Plaintiffs other than as contractors working for the government. 740 ILCS 14/25(e).

As an independent matter, Plaintiffs admit in their opposition that the only information about Plaintiffs that Defendants analyzed and shared with their customers was information "calculated from facial vectors and measurements *taken from the booking photo"* itself—that is, information contained in government records that are public. (Opp. at 18, emphasis added.) The First Amendment prohibits Plaintiffs' effort to penalize Defendants for analyzing government-published information and sharing that analysis with their customers. For that reason too, summary judgment should be entered in favor of Defendants.

Plaintiffs Misstate The Legal Standards

Plaintiffs misstate the applicable legal framework in three important ways:

First, Plaintiffs argue repeatedly that Defendants have "fail[ed] to meet their burden to preclude a question of fact." (*Id.* at 12; *see also id.* at 4, 14.) That gets Rule 56 backward. Plaintiffs, who bear the burden of proving their claims, must come forward on summary judgment with "evidence upon which a jury could properly proceed to find a verdict in [their] favor." *Modrowski v. Pigatto*, 712 F.3d 1166, 1168–69 (7th Cir. 2013) (internal quotations and citation omitted). Where a plaintiff lacks such evidence, a defendant need not "disprove" a plaintiff's claim. *See Sterk v. Redbox Automated Retail, LLC*, 770 F.3d 618, 627 (7th Cir. 2014). Plaintiffs' burden

[1] Plaintiffs could have specifically noticed the Prominvestbank and Speedway PD contracts as topics in the Rule 30(b)(6) deposition and asked Defendants' corporate representative witness about them during his deposition but they chose not to do so. If they had, the testimony would have been consistent with the declaration testimony at Dkts. 141 and 142.

cannot be met with a mere "scintilla of evidence in support of [their] position," *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986), nor by "some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986).

Second, Plaintiffs appear to misunderstand that Defendants have moved for summary judgment on Plaintiffs' *individual* claims. The dispositive issue is thus whether each Plaintiff can come forward with evidence that would permit a jury to find that Defendants collected, possessed, or used information about *each individual Plaintiff* in a manner that violated BIPA. *See Cowen v. Bank United of Texas, FSB*, 70 F.3d 937, 941, 944 (7th Cir. 1995) (affirming individual summary judgment where "claim of the *named plaintiffs* lack[ed] merit"). With respect to Mr. Sanders, his individual claims under BIPA relate only to alleged facial recognition information about himself. *See* 740 ILCS 14/20. But as Defendants' witnesses have testified unrebutted, Vigilant contracted only with government customers to provide access to the booking photo gallery that contains information about Mr. Sanders. (*See e.g.*, Pls. RSOF Ex. 18, Rule 30(b)(6) Dep. Tr. at 95:22–96:2 ("[W]e never offered this product containing jail booking photos to commercial entities. It didn't occur.").) Mere sales of search tools—like LineUp—to private customers *without* booking photo gallery access do not support Mr. Sanders' individual claims. (*See* Dkt. 114, Olive Decl. ¶¶ 5–8, 12.) Meanwhile, Plaintiffs' opposition says nothing at all about Plaintiff Simmons, conceding that summary judgment should be entered on her claims.

Third, although Plaintiffs incorrectly complain that Defendants' motion is "premature," (Opp. at 4), this case had been pending for more than 20 months when Defendants moved for summary judgment, which was now nearly a year ago (Dkts. 1, 58). Plaintiffs have filed three iterations of their complaint and substituted the individual plaintiffs multiple times, all the while clinging to their false allegation about "private customers." (Dkts. 1, 6, 72.) Judge Norgle and Magistrate Judge Cummings repeatedly rejected requests by Plaintiffs to stay or defer this motion,

instead guiding the parties through Rule 56(d) discovery focused on the dispositive issues. (Dkts. 67, 71, 77, 84, 98.) That discovery included targeted document productions, depositions of Defendants' declarants supporting summary judgment, and a Rule 30(b)(6) deposition.

Having had the benefit of that substantial discovery, Plaintiffs told the Court on August 24, 2022, that "they are not seeking further discovery under Fed. R. Civ. P. 56(d)." (Dkt. 119.) Summary judgment is entirely appropriate under these circumstances.[2]

Argument

I. Plaintiffs Have Not Established Evidence That Defendants Collected Or Disseminated Information About Them Other Than As Government Contractors.

As Defendants showed, BIPA has no application to a "contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." 740 ILCS 14/25(e). The Illinois Appellate Court recently confirmed that a defendant is "exempt under section 25(e) if it is (1) a contractor (2) of a unit of government and (3) was working for that unit of government at the time it collected or disseminated biometric information." *Enriquez v. Navy Pier, Inc.*, 2022 IL App (1st) 211414-U, ¶ 19 (Sept. 27, 2022). A "contractor" is not defined in the statute, and thus takes its "ordinary meaning," which is simply "one who contracts to do work for or supply goods to another." *Id.* ¶ 20 (quoting Black's Law Dictionary (11th ed. 2019)).

There is no genuine dispute on any part of that test. Defendants have established they were acting pursuant to (1) contracts with (2) units of government, including the Wilmette PD, since (3) the time they gathered any information from the booking photos of Plaintiffs, and at all times thereafter. (*See* Mot. at 10–11.) Further, Defendants contracted only with government entities—

[2] *See In re Dairy Farmers Cheese Antitrust Litig.*, 60 F. Supp. 3d 914, 921 n.1 (N.D. Ill. 2014) (granting summary judgment after "targeted Rule 56(d) discovery").

not private parties—to provide access to the booking photo gallery where the booking photos and related information about Ms. Simmons and Mr. Sanders are stored. (*Id.* at 11.)

Plaintiffs make three arguments in opposition, but none succeeds. First, Plaintiffs argue that there "exists a genuine dispute" about whether Vigilant's contracts with police departments like Wilmette and Beaumont even "existed" (Opp. at 15), though those agreements are clear in the record. Second, Plaintiffs argue that Vigilant *might* have obtained a booking photo of Mr. Sanders in 2012, prior to the 2014 government contracts (*id*. at 11), but there is no evidence supporting that speculation. And third, Plaintiffs argue that Defendants provided "FaceSearch to private customers" (*id.* at 4–10), but this argument depends on misreading documents and conflating other products with the *booking photo gallery*, which is the only basis for Plaintiffs' claims.

Notably, Plaintiffs do *not* argue that Section 25(e) applies only to contracts with Illinois-based government entities. (*See id.* at 17 n.6; Mot. at 11–14.) Plaintiffs have thus waived any contention that contracts with non-Illinois public authorities are not covered by Section 25(e). *See C & N Corp. v. Kane*, 756 F.3d 1024, 1027 (7th Cir. 2014) (failure to make argument constituted waiver on summary judgment).[3] For each reason, the Court should enter summary judgment in favor of Defendants on Plaintiffs' individual claims.

A. Plaintiffs Do Not Establish Any Genuinely Disputed Issue About When Vigilant Began To Work Pursuant To Government Contracts

Defendants established that they have been contractors working for government authorities to provide facial recognition technology, including access to the booking photo gallery, since

[3] As Defendants established, BIPA would violate the Dormant Commerce Clause and the First Amendment if Section 25(e) were interpreted to apply only to contracts with public authorities based in Illinois, but not those outside of Illinois. (Mot. at 20–23.) Because Plaintiffs do not argue for that interpretation, the Court should avoid potential constitutional deficiencies and assume BIPA may be reasonably interpreted to apply to public authorities outside of Illinois. *See Gresham v. Peterson*, 225 F.3d 899, 908–09 (7th Cir. 2000) (declining to invalidate statute where "a reasonable interpretation . . . could render it constitutional").

before Vigilant first gathered any information from a booking photo of Mr. Sanders. (*See* Mot. at 10.) Defendants further established that they worked pursuant to such contracts from at least September 2014 through today. (*Id.* at 10–11.) Even before that, Vigilant's law enforcement customers expressed interest in purchasing facial recognition technologies and access to a gallery of booking photos. (Dkt. 113, Hodnett Decl. ¶¶ 4–5.) In discovery, Defendants produced over a thousand government contracts. (Dkt. 143, Kras Decl. ¶ 3.) In their opposition, Plaintiffs ignore that evidence and instead attempt to raise doubts about *two* contracts that Defendants highlighted in their motion—contracts with the police departments in Wilmette, Illinois and Beaumont, California. (Opp. at 15–17.) Both efforts fail.

Regarding the Wilmette PD, Vigilant's records show in black and white that the PD signed "*Accepted*" on a September 25, 2014 quotation that included several Vigilant products like "facial recognition" and a "[f]acial [r]ecognition gallery;" the PD signed an accompanying "Software Service Program" contract with Vigilant the same day. (Dkt. 114-1, at Motorola 9344; *see also id.* at 9346–53.) Plaintiffs misleadingly argue that the "contract was never executed" (Opp. at 6), but the Wilmette PD *did* execute it (Dkt. 114-1, at Motorola 9353), and Vigilant's apparent oversight in not executing it does not negate the parties' agreement.[4] Indeed, Plaintiffs themselves submitted a public record showing that the Wilmette PD *paid* Vigilant within about 60 days of signing. (Dkt. 129-20, Pls. RSOF Ex. 20 at 8.)[5] If anything more were required, Defendants' Rule 30(b)(6) witness testified unrebutted that Vigilant provided the Wilmette PD access to its biometric

[4] Parties may neglect to execute contracts, but courts still enforce them including where the parties' conduct, such as payment and performance, shows an intent to be bound. *Am. Kitchen Delights, Inc. v. Signature Foods, LLC*, No. 16-cv-08701, 2018 WL 1394032, at *5 (N.D. Ill. Mar. 20, 2018).

[5] Plaintiffs point out that the Wilmette PD ultimately paid Vigilant $900 more than the price reflected in the quotation, but they cannot explain why this would lead to the conclusion that there was no contract, as opposed to an additional charge.

technologies under the September 2014 agreement. (*See, e.g.*, Pls. RSOF Ex. 18, 30(b)(6) Tr. at 208:10–12.) There is no genuine dispute here.

The Wilmette contract predates Vigilant's acquisition of any information from the booking photo of Mr. Sanders, so nothing further is required to show that Vigilant was working as a government contractor at the relevant time. But Defendants also established that they contracted with the Beaumont, California PD in June 2014 to provide a package of "Intelligent Led Policing ("ILP") policing tools, including "FaceSearch Hosted Facial Recognition" and an "[i]mage gallery." (*See* Mot. at 5; Dkt. 116, Defs. SOF ¶ 26; Dkt. 114-2, at Motorola 9367–68.) Plaintiffs complain that Defendants attached to their motion a "Project Quotation" signed "Approved" by the Beaumont PD rather than an Enterprise Services Agreement (Opp. at 17), but they neglect to mention that Defendants *also* produced in discovery Vigilant's fully executed Enterprise Services Agreement with the Beaumont PD for the same "ILP" products, dated September 23, 2014. (Dkt. 140-2, at Motorola 50106–14.) Plaintiffs also point to a September 2022 letter from a lawyer for the Beaumont PD stating that she located no "facial recognition" contract with Vigilant in the PD's records (Dkt. 129, Pls. RSOF ¶ 26), but that, of course, is not proof that no such contract ever existed.[6] Defendants have adduced the contracts themselves and sworn testimony corroborating them. (*See, e.g.*, Dkt. 140-2; Dkt. 114-1, at Motorola 9346; Pls. RSOF Ex. 18, 30(b)(6) Tr. at 208:10–12; Dkt. 113, Hodnett Decl. ¶ 9.) Plaintiffs do not establish even a "metaphysical doubt" about them. *Matsushita*, 475 U.S. at 586.

Plaintiffs also argue in passing that Defendants' contracts with authorities like the Wilmette and Beaumont PDs do not qualify as "government contracts" because Vigilant allegedly did not

[6] The letter that Plaintiffs submitted, for example, does not indicate how long the Beaumont PD retains documents, nor whether the person who searched looked for the "ILP" package that included booking photo gallery access (the letter mentions some Vigilant products, but not ILP).

perform a "government function" or was not "under the direction or control" of those authorities. (Opp. at 9–10.) But nothing in the statute requires such a showing. 740 ILCS 14/25(e). Courts have uniformly held that a "government contractor" is simply "[a] party to a contract" with a government entity. *Enriquez,* 2022 IL App. (1st) 211414-U ¶ 20; *see also Thornley v. CDW-Government, LLC,* No. 2020-CH-0346 (Cir. Ct. Cook County, Ill. June 25, 2021) (Dkt. 115-1, Order at 4). There is thus no genuine dispute that Vigilant was a contractor working for the government at the time it acquired information from the photo of Mr. Sanders, and at all times thereafter.

B. Plaintiffs Do Not Establish Any Genuinely Disputed Issue About When Vigilant Came To Possess Information From The Photo Of Plaintiff Sanders.

Defendants also established that the first time Vigilant obtained information from a booking photo of Plaintiff Sanders was September 30, 2014, which was after Vigilant was working under contracts with police departments like the Wilmette and Beaumont PDs. (Mot. at 6; Dkt. 114, Olive Decl. ¶ 12.) In response, Plaintiffs admit that there is no "direct evidence" that Defendants obtained information from a photo of Mr. Sanders before that date. (Opp. at 14.) Plaintiffs nonetheless launch into a series of supposed "inferences" to argue that a vendor called TLO "*could have*" obtained the booking photo of Mr. Sanders and supplied it to Defendants before 2014. (*Id.*, emphasis added.) This speculation is exactly the type of "inference upon inference" reasoning that cannot meet Plaintiffs' burden. *Pactiv Corp. v. Multisorb Techs., Inc.*, No. 10-cv-461, 2012 WL 1030258, *4 (N.D. Ill. March 27, 2012).

Plaintiffs' attempted inferential chain runs as follows: (i) before 2014, Vigilant contracted with a vendor called TLO, which licensed booking photos to Vigilant (Plaintiffs allege it was 14 million photos); (ii) TLO was sold to another company in 2014, and the buyer required Vigilant to delete the photos TLO had supplied; (iii) Vigilant contracted with a new vendor, Likeness, to

supply a set of 12 million booking photos to Vigilant beginning in late September 2014; and (iv) the booking photo of Mr. Sanders was included in the set supplied by Likeness. (Opp. at 12–14.) From that, Plaintiffs surmise that because Likeness provided a set of photos that included Plaintiff Sanders, "TLO *could have* as well." (*Id.* at 14, emphasis added.)

Even on its own terms, this type of "speculation or conjecture will not defeat a summary judgment motion." *McDonald v. Village of Winnetka*, 371 F.3d 992, 1001 (7th Cir. 2004). The idea that a single person's booking photo found in one vendor's collection must also be found in another vendor's collection has no evidentiary or logical support. The FBI reports that more than *ten million* people are arrested *per year* in the United States.[7] But there is an additional problem for Plaintiffs. Defendants' corporate representative testified unrebutted that the booking photos supplied by the prior vendor, TLO, included booking photos from only *Texas* and *Florida*, not from Illinois where Plaintiffs Sanders was arrested. (*See* Pls. RSOF Ex. 18, 30(b)(6) Tr. 80:3–11, 82:10–15, 100:17–24, 103:7–11, 272:9–20.) Plaintiffs simply ignore that evidence, which forecloses their speculation.

C. Plaintiffs Do Not Establish Any Genuine Dispute About "Private Customers" For The Booking Photo Gallery.

Defendants also established that they contracted only with government authorities to provide access to the booking photo gallery that contains information about Plaintiffs. (Mot. at 11; Dkt. 116, Defs. SOF ¶ 22.) Or, as the *Enriquez* court put it, Defendants were continuously "working for [a] unit of government at the time [they] collected or disseminated biometric information." 2022 IL App. (1st) 211414-U ¶ 19.

[7] *2019 Crime in the United States, Estimated Number of Arrests*, https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/tables/table-29.

Plaintiffs do not quarrel with Defendants' more than one thousand contracts with government entities, nor assert that there was some period in which Defendants did not have active government contracts. Instead, Plaintiffs argue that Defendants "sold FaceSearch to private customers" in addition to government entities. (Opp. at 6–7.) Plaintiffs rely on three types of documents to make this argument: (1) documents that mention sales of some facial recognition products to private customers *but not access to the booking photo gallery*; (2) a reference to a sale to a customer called Prominvestbank; and (3) a reference to a sale to the Speedway, Indiana PD financed by the Indianapolis Motor Speedway. (*See id.*; *see also* Pls. RSOF ¶ 22.) In fact, none of those materials supports Plaintiffs' claims.

1. There is no genuine dispute that Vigilant contracted only with government entitles for access to the booking photo gallery.

Plaintiffs' argument depends on conflating separate aspects of products offered by Vigilant—*i.e.*: (a) technologies like FaceSearch, a "tool to quickly and efficiently search through . . . photos"; and (b) *the booking photo gallery*, which is a compilation of "publicly available booking photos" and information drawn from those photos. (Dkt. 113, Hodnett Decl. ¶¶ 4–5.) In other words, the search *tool* is not the same as the *collection of photos* to be searched. Thus, while Vigilant's government customers can use Vigilant's tools to search pictures in the booking photo gallery, Vigilant's private customers can search only their own "watchlists" of photos that they compile themselves, *not* the booking photo gallery. (*See* Dkt. 114, Olive Decl. ¶ 8.) Plaintiffs deposed Defendants' witnesses, and each testified under oath that Defendants contracted only with government entities to provide access to the booking photo gallery. (*See, e.g.*, Pls. RSOF Ex. 18, 30(b)(6) Tr. at 98:9–13.) Plaintiffs nowhere address that unrebutted testimony.

Instead, Plaintiffs rely on a handful of pages from Vigilant's marketing materials that primarily refer to Vigilant's sales of facial recognition *tools*, but not access to the *booking photo*

gallery that contains Plaintiffs' photos and information. (*See* Opp. at 6–7; *see also* Pls. RSOF ¶¶ 7, 11, 15, 22.) Those documents are entirely consistent with Defendants' submissions and testimony. For example, a 2014 presentation about Vigilant's "facial recognition" products notes that Vigilant has "law enforcement" customers as well as customers in "banking, casinos, [and] retail." (Dkt. 129-1, Pls. RSOF Ex. 1 at Motorola 44260.) That is true and unremarkable. Vigilant sold some facial recognition tools to private customers, but *not* access to the booking photo gallery. (*See* Dkt. 114, Olive Decl. ¶ 8; Dkt. Pls. RSOF Ex. 18, 30(b)(6) Tr. at 95:22–96:2.) Other marketing materials geared toward public safety customers note that products like FaceSearch could be sold with access to booking photos included (*e.g.*, Dkt. 129-2 Pls. RSOF Ex. 2 at Motorola 50277,) but, again, the undisputed evidence is that Defendants made no such combined sales to private customers. Even further afield are Plaintiffs' references to marketing documents that describe other Vigilant products, such as license plate recognition ("LPR") technology. (*See, e.g.*, Dkt. 129-2, Pls. RSOF Ex. 2 at Motorola 50280 ("LPR Provider for US Lenders"); Dkt. 129-4, Pls. RSOF Ex. 4 at Motorola 50201 (same); *id.* at 50214 (discussion of LPR product).) These have nothing to do with facial recognition, and much less the booking photo gallery.

Plaintiffs also point to "reseller agreements" between Vigilant and third-party resellers, which mention "Commercial" and "Casino" as well as "Public Safety" markets. (Opp. at 7.) Plaintiffs, however, omit that those agreements cover a dozen different Vigilant products, many of which do not involve facial recognition at all, such as "L[icense] P[late] R[eader] Camera Kits" and "CarDetector" software. (*See* Dkt. 129-14, Pls. RSOF Ex. 14 at Motorola 43270; Dkt. 129-15, Pls. RSOF Ex. 15 at Motorola 43733; *see also* Dkt. 114, Olive Decl. ¶ 8.)[8] There is thus nothing

[8] Further, those agreements expressly required that all sales be formalized in a contract executed between the end-user and Vigilant, giving Vigilant the ultimate control over which customers could purchase which products. (Dkt. 129-14, Pls. RSOF Ex. 14 at Motorola 43262, ¶ 5.7; Dkt. 129-15, Pls. RSOF Ex. 15 at Motorola 43725, ¶ 5.7.)

in these documents that is inconsistent with Defendants' testimony and submissions—*i.e.*, Vigilant offered a menu of products to government and non-government customers, but it did not contract with any non-government customers to provide access to the booking photo gallery, which is the only basis for Plaintiffs' claims.

2. There is no genuine dispute regarding Prominvestbank or the Indianapolis Motor Speedway.

When it comes to actually identifying any supposed "private customer" that purchased access to the booking photo gallery, Plaintiffs come up with only two alleged buyers: a Ukrainian bank called Prominvestbank, and the company that owns the Indianapolis Motor Speedway. (Opp. at 7; Dkt. 129, Pls. RSOF ¶¶ 15, 22.) Plaintiffs are wrong on both.

With respect to Prominvestbank, Plaintiffs again conflate Vigilant's search tools with the booking photo gallery. Prominvestbank purchased a tool called "LineUp" from Vigilant, which allowed it to search its own "watchlist" gallery of photos, not the booking photo gallery. (Dkt. 141, Garoutte Decl. ¶¶ 6–7.) As Defendants' witnesses have averred unrebutted, commercial customers that purchase LineUp cannot search the booking photo gallery. (*Id.*; Dkt. 114, Olive Decl. ¶ 8; Dkt. Pls. RSOF Ex. 18, 30(b)(6) Tr. at 97:15–19.) Plaintiffs do not identify any contrary proof. They refer only to one line on a spreadsheet that lists Prominvestbank and licenses for "LineUp/FaceSearch" (Dkt. 129-13, Pls. RSOF Ex. 13), but, as noted, those products can be used *without* the booking photo gallery. That is exactly the case here. (Dkt. 141, Garoutte Decl. ¶¶ 6–7.)

Plaintiffs are also mistaken with respect to the Indianapolis Motor Speedway. Plaintiffs refer to spreadsheet entries relating to a sale in March 2017 involving the "Hulman Motor Sports Speedway," which Plaintiffs categorize as a "private" sale. (Opp. at 7; Dkt. 129, Pls. RSOF ¶ 22.) But Plaintiffs again misinterpret. The contract associated with the sale reflected in the spreadsheet

was between Vigilant and the *police department* in Speedway, Indiana, where the Motor Speedway is located. (*See* Dkt. 140-1 at Motorola 8419.) Vigilant contracted to provide access to the booking photo gallery only to the Speedway PD, not the owner of the racetrack. (Dkt. 142, Workman Decl. ¶¶ 3–4.) That owner, Hulman Motorsports, paid for the Speedway, Indiana PD's purchase of Vigilant products, but it was not a party to the contract and never contracted for access to the booking photo gallery. (*Id.* ¶ 3.) Other than the misinterpreted spreadsheet, Plaintiffs do not (and cannot) point to any contrary evidence. Thus, again, Vigilant was acting pursuant to a "contract[]" with a "local unit of government" with respect to the Indianapolis Motor Speedway. 740 ILCS 14/25(e).

At bottom, Plaintiffs fail to "present definite, competent evidence to rebut the motion." *Michael v. St. Joseph County*, 259 F.3d 842, 845 (7th Cir. 2001). Summary judgment should be entered in favor of Defendants on Plaintiffs' individual claims.

II. Each Individual Plaintiff's Claims Are Precluded By The First Amendment.

As an independent matter, Plaintiffs' claims are precluded by the First Amendment. Plaintiffs' claims are unprecedented. They seek to hold Defendants liable for a core First Amendment activity: analyzing information disclosed *by the government in public records* and communicating the results of that analysis to others. Plaintiffs admit that Defendants make use only of information that the government itself makes public—that is, "facial vectors and measurements *taken from the booking photo*" that the government elects to publish. (Opp. at 18, emphasis added.) Plaintiffs do not identify any BIPA case similarly targeting the analysis of public government records. Nor do Plaintiffs identify *any* authority in *any* context upholding an effort to penalize a party for analyzing information freely published by public authorities. Any such effort would contravene the long-established "privilege to publish matters contained in public records

even if publication would offend the sensibilities of a reasonable person." *Willan v. Columbia Cty.*, 280 F.3d 1160, 1163 (7th Cir. 2002).

Plaintiffs make three arguments seeking to avoid the First Amendment. First, they argue that Defendants "create a new representation" of information not fully protected by the First Amendment. (Opp. at 18.) Second, Plaintiffs cite BIPA cases that *did not concern public records* to argue that strict scrutiny should not apply. (*Id.* at 22–23.) Third, Plaintiffs argue that BIPA satisfies "intermediate scrutiny." (*Id.* at 24–26.) Each argument fails.

A. Analyzing Government-Published Records And Communicating That Analysis Is Speech Strictly Protected By The First Amendment.

Plaintiffs first argue that Defendants do not "simply republish[] publicly available information," but, instead "generate[] non-public, biometric information that does not enjoy robust First Amendment protection." (Opp. at 18–19.) Plaintiffs, however, misunderstand the law and mischaracterize the undisputed facts.

With respect to the law, the First Amendment protects Defendants without regard to whether Plaintiffs characterize Defendants' analysis of public booking photos as "republishing" information gleaned from those photos or "creat[ing] a new representation" of information based on those same public records. As Defendants established (Mot. at 15–16), the First Amendment protects the "*creation and dissemination of information*." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011) (emphasis added). That protection extends to even "dry" information, such as an analysis of drug prescription records by "data miners," *id.* at 558, 570, scientific samples of natural resources, *Western Watersheds Project v. Michael*, 869 F.3d 1189, 1197 (10th Cir. 2017), and telephone directories, *Dex Media W., Inc. v. City of Seattle*, 696 F.3d 952, 954 (9th Cir. 2012). The Supreme Court has recognized "the *rule* that information is speech," including because "[f]acts, after all, are the beginning point for much of the speech that is most essential to advance human

knowledge and to conduct human affairs." *Sorrell*, 564 U.S. at 570–71 (emphasis added). Thus, even assuming Defendants "generate" information, the First Amendment protects the "creation and dissemination" of that information in all events. *Id.* at 570.

Moreover, it is undisputed that the only *source* of information about Plaintiffs that Defendants utilized for their analysis is information freely published by the government. Plaintiffs themselves admit that Defendants analyzed only "data points" and "measurements *taken from the [public] booking photo*" *itself, i.e.*, information that appears in the very document the state statutorily elected to make public. (Opp. at 18, emphasis added); *see also* 5 ILCS 160/4a(a)(1).[9] Plaintiffs accuse Defendants of transforming that public information into a "new representation" (Opp. at 18), but the First Amendment protects the *use* of government-published information to develop expression, including in new and unanticipated ways. Sifting through information made public by the government, analyzing it, highlighting parts of it—and even developing "new representations" of it—all lie at the core of the First Amendment's protections. *See, e.g.*, *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 472–73, 496–97 (1975) (information uncovered from "examination of the indictments" in courthouse files was strictly protected); *Nieman v. VersusLaw, Inc.*, 512 Fed. Appx. 635, 636–37 (7th Cir. 2013) (same, internet search engines linked and "index[ed]" litigation records); *Vrdolyak v. Avvo, Inc.*, 206 F. Supp. 3d 1384, 1385–86, 1389 (N.D. Ill. 2016) (same, ratings of lawyers constructed from "information gleaned from public records").[10]

[9] In their response to Defendants' LR 56.1 statement, Plaintiffs purport to "deny" the fact that "FaceSearch does not use any information about a person's face that is not contained in the photo itself," but the only basis for that "denial" is Plaintiffs' assertion that "FaceSearch *creates* a new digital representation." (Dkt. 129, Pls. RSOF ¶ 20, emphasis added.) That argument, however, concerns the *output* of Defendants' analysis, not the *source* of information that Defendants use.

[10] Illinois has made booking photos freely public for decades, if not longer. *E.g.*, *People v. Gendron*, 243 N.E.2d 208, 210 (1968) (noting publication of "mug shot"). Restricting how the public can analyze and utilize information the government chooses to make public cannot be squared with principles of free speech.

In response, Plaintiffs cite to off-point cases that considered whether companies that analyze photos of faces are exempt from BIPA because "photograph[s]" are excluded from BIPA's definition of "biometric identifier." (*See* Opp. at 19.) But that has nothing to do with the First Amendment issue here. Even assuming that an analysis of a photo is subject to BIPA, it remains undisputed that the only photos analyzed here were government-published records, made freely public by law. Where a state chooses to "plac[e] the information in the public domain," the state "must be presumed to have concluded that the public interest was thereby being served." *Cox Broadcasting*, 420 U.S. at 495. None of Plaintiffs' authorities concern the context of information published by the government. For each reason, the First Amendment fully protects Defendants' expressive activity in analyzing public records and communicating that analysis to others.

B. Strict Scrutiny Applies And Precludes Plaintiffs' Claims.

1. Plaintiffs' claims represent a content-based restriction on speech.

As Defendants also established, the First Amendment requires that Plaintiffs' claims be analyzed under the strict scrutiny standard because they target the use of a particular type of information—*i.e.*, information categorized as "biometric" under BIPA. (Mot. at 17–19.) Here, where the information at issue is derived exclusively from government-published records, Plaintiffs cannot establish that the application of BIPA is "narrowly tailored to serve compelling state interests." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015).

In response, Plaintiffs first argue that BIPA is not subject to strict scrutiny because the statute supposedly is not "content based." (Opp. at 23–24.) But the statute, on its face, restricts the collection and dissemination of a specifically defined *type* of information: "biometric information" and "biometric identifiers," and it defines each in detail. 740 ILCS 14/10. For example, a "scan of hand or face geometry" is restricted, but a "photograph" is not. *Id.* Information used to "treat an illness" is excluded from restriction, but the same information used for some other purpose is not.

Id. These are textbook content-based distinctions. The statute both "defin[es] regulated speech by particular subject matter," *i.e.*, "biometric information," *and* "defin[es] regulated speech by its function or purpose," *i.e.*, "information used to identify an individual." *Reed*, 576 U.S. at 163; *see also* 740 ILCS 14/10. Plaintiffs argue that BIPA does not regulate any particular viewpoint about biometrics, but that is not the test for strict scrutiny. "[A] speech regulation targeted at a specific subject matter *is content based* even if it does not discriminate among viewpoints within that subject matter." *Reed*, 576 U.S. at 169 (emphasis added).[11]

Plaintiffs next argue that BIPA's application in this case is not subject to strict scrutiny because the statute purportedly regulates "nonspeech" activities, which Plaintiffs characterize as "harvesting" biometric information. (Opp. at 20–22.) For this argument, Plaintiffs rely on three cases from other courts in this district.[12] Critically, however, none of those cases concerned the use of *government-published information*, like the booking photos at issue here.[13] Analyzing information that the government makes freely public is a core First Amendment activity; there is no legal authority deeming such conduct "nonspeech." Indeed, the Supreme Court has cautioned that courts do not have "freewheeling authority to declare new categories of speech outside the scope of the First Amendment." *United States v. Stevens*, 559 U.S. 460, 472 (2010).

---

[11] And "[a] law that is content based on its face is subject to strict scrutiny regardless of the government's benign motive, content-neutral justification, or lack of animus" toward a particular view. *Id.* at 165. Plaintiffs quote *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452 (Ill. Cir. Ct. Aug. 27, 2021) for the proposition that BIPA is not content based because it does not treat biometric information of "people yelling" differently from that of "people smiling," but that is exactly the type of analysis rejected in *Reed*. 576 U.S. at 169.

[12] *Wilk v. Brainshark, Inc.*, No. 21-cv-4794, 2022 WL 4482842 (N.D. Ill. Sept. 27, 2022) (Blakey, J.); *Sosa v. Onfido, Inc.*, No. 20-cv-4247, 2022 WL 1211506 (N.D. Ill. Apr. 25, 2022) (Aspen, J.); *In re Clearview AI Consumer Priv. Litig.*, 585 F. Supp. 3d 1111(N.D. Ill. 2022) (Coleman, J).

[13] *Clearview* involved an allegation that a company "covertly scraped" billions of images from internet websites, and *Wilk* and *Sosa* involved companies that allegedly obtained non-public images of faces uploaded by users. *Clearview*, 585 F. Supp. 3d at 1120; *Wilk*, 2022 WL 4482842, at *1; *Sosa*, 2022 WL 1211506 at *1.

Plaintiffs' cases are further inapt in that each one relied on *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937 (7th Cir. 2015), a case that concerned a federal law prohibiting parties from "obtain[ing] or disclos[ing] personal information" from state motor vehicle records. *Id.* at 941; *see also* 18 U.S.C. § 2722(a). The Seventh Circuit held that the ban on "obtaining" such information did not violate the First Amendment because it was "a limitation only on *access* to information" held by the government, and "[t]here is no constitutional right to have access to particular government information." *Id.* at 947 (internal quotations and citations omitted). In the cases cited by Plaintiffs, the district courts relied on *Dahlstrom* to find that BIPA "only restrict[s] how a private entity may *access* someone's biometric information," *Wilk*, 2022 WL 4482842, at *7, which the courts held "is not a restriction on speech," *Sosa*, 2022 WL 1211506 at *13. But here again, unlike in *Dahlstrom*, Defendants have not accessed any information held by the government; they have analyzed information that the government itself made fully public. *Wilk* and *Sosa* are further off-point because the defendant in each case did not identify any "speech it wish[ed] to undertake" by analyzing alleged biometric information. *Sosa*, 2022 WL 1211506, at *14; *see also Wilk*, 2022 WL 4482842, at *7–8. Here, in contrast, it is undisputed that Defendants analyze booking photos in order to *communicate* their analysis to their customers.

In short, Plaintiffs' claims represent a content-based effort to penalize Defendants' analysis of public government records and their communication of that analysis to their clients. The only applicable standard in those circumstances is strict scrutiny.

2. The application of BIPA in this case does not withstand strict scrutiny.

As Defendants also established (Mot. at 17–19), applying BIPA here cannot survive strict scrutiny. Under a strict scrutiny framework, a restriction on the dissemination of information must be "narrowly tailored to serve compelling state interests." *Reed*, 576 U.S. at 163.

Plaintiffs argue in response that protecting privacy is an "important government interest" (Opp. at 24), but that interest has reduced salience where Illinois has already elected to make Plaintiffs' booking photos, and the information contained within them, freely public. 5 ILCS 160/4a(a)(1). Privacy is often identified as the justification for restrictions on information, but that interest gives way where the state makes the information public, even if in a limited or inadvertent manner. *See, e.g.*, *Fla. Star v. B.J.R.*, 491 U.S. 524, 538 (1989) (First Amendment overrode privacy considerations where police "erroneous[ly]" included information in report made available to press); *Cox*, 420 U.S. at 472–73; *Nieman*, 512 F. Appx. at 636.

In any event, Plaintiffs do not even attempt to argue that BIPA is "narrowly tailored" to advance a compelling privacy interest here, because it is not. Where the government itself puts information in the public domain, "a less drastic means than punishing truthful publication almost always exists for guarding against the dissemination of private facts." *Fla. Star*, 491 at 534. Illinois could choose not to publish booking photos, or it could exempt from BIPA's coverage information that may be discerned from records the state itself chooses to make public. Making the records public and then punishing the analysis of those records does not fit any concept of narrow tailoring. Plaintiffs' claims are thus precluded by the First Amendment.

C. Plaintiffs' Claims Do Not Survive Even Intermediate Scrutiny.

Rather than address the strict scrutiny standard, Plaintiffs primarily argue that their claims are subject only to intermediate scrutiny. (Opp. at 24.) But even if intermediate scrutiny applied, Plaintiffs' claims remain precluded by the First Amendment. To pass that test, the government interest in regulating speech (1) must be substantial, (2) the regulation must advance that interest; and (3) the regulation must be narrowly drawn. *See Pearson v. Edgar*, 153 F.3d 397, 401 (7th Cir. 1998). The Seventh Circuit analyzes the second and third prongs together, asking if there is a

"reasonable fit" between the restriction and the "goal to be achieved" by the restriction. *Id.* at 402. Plaintiffs' claims, however, satisfy none of those requirements.

First, a purported interest in privacy has, at best, a reduced weight in the context of information contained in government-published records such as booking photos. None of the decisions relied upon by Plaintiffs concerned this special factual circumstance. Second, there is no "reasonable fit" between BIPA's restrictions as applied to Defendants and protecting privacy where the information at issue was contained in government-published records. Any "fit" is further compromised by BIPA's exceptions for the banking and healthcare sectors. For each reason, even if intermediate scrutiny applies, Plaintiffs' claims are barred by the First Amendment.

III. Summary Judgment Is Appropriate On Each Plaintiff's Unjust Enrichment Claim.

Plaintiffs concede that their unjust enrichment claim is derivative of their BIPA claims. (Opp. at 28.) Summary judgment is thus appropriate on this claim for the reasons above.

Conclusion

For the reasons stated herein, Defendants respectfully request summary judgment in their favor on all of Plaintiffs' individual claims and dismiss all of those claims with prejudice.

Dated: November 14, 2022

Respectfully submitted,

DEFENDANTS MOTOROLA SOLUTIONS, INC. AND VIGILANT SOLUTIONS, LLC

By: */s/ David C. Layden*
One of their attorneys

David C. Layden
dlayden@jenner.com
Andrew W. Vail
avail@jenner.com
JENNER & BLOCK LLP
353 North Clark Street
Chicago, Illinois 60654
312-840-8688